REMARKS

Claims 1-17 and 21-22 are pending for examination with claims 1, 2, 3, 5, 6, 8, 9, 10, 11, 17, and 21 being independent claims. Applicant has amended claims 1-5, 7, 11, and 17 to correct minor grammatical mistakes, and not for any reasons of patentability. The scope of the amended claims remains unchanged. No new matter has been added.

Initially, the undersigned wishes to thank Examiner Parthasarathy for the courtesies extended in granting and conducting a telephone interview on April 11, 2005. The substance of the telephone interview briefly introduced the arguments discussed more fully below with reference to claim 1.

Rejections under 35 USC § 103

Claims 1-8, 14-15 and 20-21 stand rejected under 35 USC § 102(e) as being unpatentable over U.S. Patent No. Re. 36,946 to Diffie et al. [hereinafter Diffie]. Applicant respectfully traverses the rejection as follows.

Diffie is directed towards providing a secure wireless communication link between a mobile nomadic device and a base computing unit. (*See*, Diffie, Abstract). More particularly, the privacy and authentication system described in Diffie teaches that a mobile unit sends to the base a host certificate (Cert_Mobile). In response, the host sends to the host a base certificate (Cert_Base), a first random number (RN1) encrypted in the mobile's public key, and a digital signature using the private key of the base. The host then responds with a second random number (RN2) encrypted in the mobile's public key, and a digital signature using the private key of the mobile. (*See*, Diffie, col. 7, line 38-col. 8, line 52). The host certificate contains the mobile public key and is

signed by a certification authority; and similarly, the base certificate contains the public key of the base and is signed by a certification authority. (*See*, Diffie, col. 7, lines 6-10).

Independent Claim 1

Claim 1 recites, *inter alia*, the network address having a portion derived from the public key of the first computing device. Diffie does not teach or suggest these features of claim 1. More particularly, Diffie does not teach or suggest, much less even mention a network address to route the exchanged messages. Rather, Applicant cannot find any reference in Diffie which suggests a network address, much less, that a portion of the network address may be derived from the public key of any computing device, much less derived from the public key of the first computing device.

In the telephone interview of April 11, 2005, Examiner Parthasarathy suggested that the encryption of the first random number by the mobile public key was a network address. Applicant respectfully disagrees. Specifically, any value contained in a message is not a network address. Applicant's specification at paragraph 004, states that "In network communications, an often used form of identity is the network address used by a device to identify itself on the network." Thus, the network address is a form of identity used to identify a device on the network. Moreover, Applicant's specification at paragraphs 0032 and 0033 discusses one example of a network address with reference to protocol of IPv6 and states that modern network addresses typically contain a routable address that can be used to route a message to an appropriate network link. In this manner, a network address identifies a device and is used to route information to the device, and is often governed by some network address protocol such as IPv6. There is nothing in Diffie which teaches or suggests a network address, much less a

network address having a portion derived from the public key of a first computing device.

Moreover, assuming without agreeing that Diffie's encryption of the first random number is a network address, this encryption is not derived from the public key of a first computing device. In the interview, Examiner Parthasarathy suggested that Diffie's inclusion of E(Pub_Mobile, RN1)(*see*, Diffie, col. 8, line 8) was an encryption of the mobile device's public key (Pub_Mobile) by a key RN1, and that the result was a derivation of the public key of the mobile device. Applicant respectfully disagrees. Diffie specifically states that the notation of E(X, Y) is defined as "the encryption of Y under key X." (Diffie, col. 6, line 39). In this manner, the random number is encrypted *by* the public key of the mobile host. Thus, the encrypted first random number is not derived *from* the public key, but is rather derived from the first random number.

In addition, claim 1 recites, *inter alia*, the message including the digital signature in a packet option. Diffie does not teach or suggest these features of claim 1. Rather, Diffie is silent as to the format of the messages exchanged between the mobile host and the base. More particularly, Diffie is silent as to whether the information in the exchanged massages are included in one or more message headers, the message body, and the like. In contrast, claim 1 specifically recites that the message includes the digital signature in a packet option, which allows the recipient of the message to discard the signature in the packet option and accept the remainder of the message. (*See*, specification, para. 0039). Diffie does not teach or suggest the specific features of claim 1, nor even suggest the functionality of a packet option.

Accordingly, claim 1 distinguishes over Diffie such that the rejection under § 102 should be withdrawn.

Independent Claim 2

Claim 2 recites, *inter alia*, a computer readable medium containing instructions for performing a method which is identical to that claimed in claim 1. As a result, claim 2 distinguishes over Diffie for at least the foregoing reasons discussed above with reference to claim 1. Accordingly, Applicant respectfully requests withdrawal of the rejection under § 102.

Independent Claim 3

Claim 3 recites, *inter alia*, deriving a portion of a second network address from the public key of the first computing device. As discussed above with reference to claim 1, Diffie does not teach or suggest a network address, much less a second network address having a portion derived from the public key of a first computing device. Moreover, even were an encryption of a random number a network address, such encryption of a random number *by* a public key of the mobile device is not derived *from* the public key.

Accordingly, claim 3 distinguishes over Diffie such that the rejection under § 102 should be withdrawn. Claim 4 depends from claim 3, and is patentable for at least the foregoing reasons.

Independent Claim 5

Claim 5 recites, *inter alia*, a computer readable medium containing instructions for performing a method which is identical to that claimed in claim 3. As a result, claim 5 distinguishes over Diffie for at least the foregoing reasons discussed above with reference to claim 3. Accordingly, Applicant respectfully requests withdrawal of the rejection under § 102.

Independent Claim 6

Claim 6 recites, *inter alia*, a method for a computing device to derive a node-selectable portion of a network address and setting the node-selectable portion of the network address to a portion of the value produced by the hashing. As discussed above with reference to claim 1, Diffie does not teach or suggest a network address. Moreover, Diffie does not teach or suggest a method of deriving a network address, much less deriving a node-selectable portion of a network address, and even much less setting the node-selectable portion of the network address to a portion of the value produces by the hashing as recited in claim 1.

Claim 6 also recites, *inter alia*, comparing a portion of a value produced by the hashing of a public key with a portion of the network address other than the node-selectable portion. As discussed above with reference to claim 1, Diffie does not teach or suggest a network address. Moreover, Diffie does not teach or suggest comparing anything to a network address, much less comparing a portion of a value produced by hashing the public key to a network address. Even were Diffie to suggest comparing a hash of the public key with a network address, there is nothing in Diffie to teach or suggest that a portion of a hashed public key is compared to the portion of the network address that is not *node-selectable*.

Claim 6 recites, *inter alia*, if the portions do not match, choosing a modifier, appending the modifier to the public key, and repeating the hashing and comparing. Applicant is unable to find any reference in the cited sections of Diffie which teach or suggest these features of claim 6. Rather, Diffie does suggest that the certificate contains a hash of the public key (*see*, Diffie, col. 7, lines 23-37) and does suggest that randomly generate numbers, such as CH1, RN1, and RN2 may be included in a message.

However, none of the random numbers of Diffie is appended to the public key, much less hashed together, and even much less compared again to the portion of the network address other than the node-selectable portion.

Accordingly, claim 6 distinguishes over Diffie such that the rejection under § 102 should be withdrawn. Claims 7-8 depend from claim 6, and are patentable for at least the foregoing reasons.

Independent Claim 9

Claim 9 recites, *inter alia*, a method for a computing device to derive a node-selectable portion of a network address from a public key of the computing device and from a route prefix of the network address of the computing device. As discussed above with reference to claim 1 and 6, Diffie does not teach or suggest a network address, much less a method for deriving a network address, and even much less deriving a network address from a public key.

Claim 9 recites, *inter alia*, hashing the public key and at least a portion of the route prefix of the network address. Diffie does not teach or suggest hashing any portion of a network address, much less hashing the outré prefix of the network address, and much less hashing the route portion of the network prefix with a public key.

Claim 9 recites, *inter alia*, setting the node-selectable portion of the network address to a portion of the value produced by the hashing. As discussed above with reference to claim 6, Diffie does not teach setting a network value to anything, much less setting the node-selected portion of a network address, and much less setting the node-selectable portion of the network address to a portion of a hashed value.

Claim 9 recites, *inter alia*, checking to see if the network address is already in use, and if so, choosing a modifier, appending the modifier to the public key, and repeating the hashing, setting, and checking. Diffie does not teach or suggest anything about network addresses, much less checking to see if there is an already existing network address. Moreover, as discussed above with reference to claim 6, Diffie does not teach or suggest selecting a modifier, appending the modifier to the public key, and hashing the combined public key and modifier.

Accordingly, claim 9 distinguishes over Diffie such that the rejection under § 102 should be withdrawn. Claim 10 depends from claim 9, and is patentable for at least the foregoing reasons.

Independent Claim 11

Claim 11 recites, *inter alia*, deriving a portion of a second network address from the public key of the first computing device. As discussed above with reference to claim 1, Diffie does not teach or suggest a network address, much less deriving a portion of a second network address from the public key of the first computing device. Moreover, even were an encryption of a random number a network address, such encryption of a random number *by* a public key of the mobile device is not derived *from* the public key.

Claim 11 recites, *inter alia*, caching the public key in association with the first network address if the derived portion of the second network address matches a corresponding portion of the first network address. Diffie does not teach or suggest these features of claim 11. Rather, Diffie does not compare anything to a network address of a sending device, and as such cannot do anything (much less cache the public key) in response to a match between the derived portion of the second network address and a corresponding portion of the first network address.

Accordingly, claim 11 distinguishes over Diffie such that the rejection under § 102 should be withdrawn. Claims 12-17 depend from claim 11, and are patentable for at least the foregoing reasons.

Independent Claim 17

Claim 17 recites, *inter alia*, a computer readable medium containing instructions for performing a method which is identical to that claimed in claim 11. As a result, claim 17 distinguishes over Diffie for at least the foregoing reasons discussed above with reference to claim 11. Accordingly, Applicant respectfully requests withdrawal of the rejection under § 102.

Independent Claim 21

Claim 21 recites, *inter alia*, the network address derived, at least in part, from a hash of the public key. As discussed above with reference to claim 1, Diffie does not teach or suggest a network address, much less deriving at least a part of the network address from the public key, and even much less deriving at least a part of the network address from a hash of the public key. Moreover, even were an encryption of a random number a network address, such encryption of a random number *by* a public key of the mobile device is not derived *from* the public key, and is not derived from a *hash* of the public key.

Accordingly, claim 21 distinguishes over Diffie such that the rejection under § 102 should be withdrawn. Claim 22 depends from claim 21, and is patentable for at least the foregoing reasons.

CONCLUSION

Accordingly, in view of the above amendment and remarks it is submitted that the claims are patentably distinct over the prior art and that all the rejections to the claims have been overcome. Reconsideration and reexamination of the above Application is requested. Based on the foregoing, Applicants respectfully requests that the pending claims be allowed, and that a timely Notice of Allowance be issued in this case. If the Examiner believes, after this amendment, that the application is not in condition for allowance, the Examiner is requested to call the Applicant's attorney at the telephone number listed below.

If this response is not considered timely filed and if a request for an extension of time is otherwise absent, Applicants hereby request any necessary extension of time. If there is a fee occasioned by this response, including an extension fee that is not covered by an enclosed check please charge any deficiency to Deposit Account No. 50-0463.

Respectfully submitted,

Microsoft Corporation

Date: 4/20/05

By: _____

Carole A. Boelitz, Reg. No.: 48,958
Attorney for Applicants
Direct telephone (425) 722-6035
Microsoft Corporation
One Microsoft Way
Redmond WA 98052-6399

CERTIFICATE OF MAILING OR TRANSMISSION [37 CFR 1.8(a)]

I hereby certify that this correspondence is being:

☒ deposited with the United States Postal Service on the date shown below with sufficient postage as first class mail in an envelope addressed to: **Mail Stop AF**, Commissioner for Patents, P. O. Box 1450, Alexandria, VA 22313-1450

☐ transmitted by facsimile on the date shown below to the United States Patent and Trademark Office at (703) _____.

4/20/05
Date

_____
Signature

Carole A. Boelitz

Type of Response: Response
Application Number: 10/010,352
Attorney Docket Number: 171135.02
Filing Date: 11/13/2001